UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/603,209	06/25/2003	Ulrich Emmerling	071308.0443	2679

31625 7590 12/09/2008

BAKER BOTTS L.L.P.
PATENT DEPARTMENT
98 SAN JACINTO BLVD., SUITE 1500
AUSTIN, TX 78701-4039

EXAMINER	
DWIVEDI, MAHESH H	
ART UNIT	**PAPER NUMBER**
2168	

MAIL DATE	DELIVERY MODE
12/09/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/603,209	EMMERLING ET AL.	
	Examiner	Art Unit	
	MAHESH H. DWIVEDI	2168	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 November 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-17* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-17* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 June 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☒ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 11/18/2008 has been entered.

Remarks

2. Receipt of Applicant's Amendment, filed on 11/18/2008, is acknowledged. The amended parts include the amending of claims 1, and 11.

Priority

3. Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

5. Claims 1 and 11 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. Specifically, the amended limitations "and providing no further communication between the first object and the at least one further object" is explicitly nor implicitly found in the applicant's suggested area of support in the specification (Page 5, lines 13-26 and Figure 1) nor anywhere else in the specification. There is no mention of the negative limitation of not providing anymore communication between the first object and the at least one further object. Moreover, the specification of the instant

application states that “With a key activated in this way actions such as unlocking or locking the central locking and deactivating or activating the vehicle immobiliser, "activating or deactivating the vehicle security etc. can be activated for transmission procedures known for passive access systems after authorization or authentication has taken place” (Page 9, lines 10-13). To the contrary of the aforementioned amendment, there are further transmissions between the first object and the at least one other object via the “can be activated for transmission procedures known for passive access systems”.

6. Claims 2-10 and 12-17 are rejected for incorporating the deficiencies of independent claims 1 and 11.

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claim 11 recites the limitation "and providing no further communication between **the first object** and **the at least one further object**" in page 4. There is insufficient antecedent basis for this limitation in the claim, as there is no previous mentioned of “the first object” and “the at least one further object" in the claim.

9. Claims 12-17 are rejected for incorporating the deficiencies of independent claim 11.

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation

under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

12. Claims 1-2, 10-11, and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Stellberger** (U.S. Patent 4,509,093) and in view of **Schwegler et al.** (U.S. Patent 5,808372).

Regarding claim 1, **Stellberger** teaches a method comprising:

A) transmitting an item of information unidirectionally between the first object and the at least one further object (Column 6, lines 60-67-Column 7, lines 1-8);

C) calculating a computation result in the relevant receiving object from parts of the transmitted information (Column 7, lines 9-23);

D) comparing the calculated computation result with a computation result transferred with the information in the relevant receiving object (Column 4, lines 22-27, Column 9, lines 32-36); and

E) authenticating the first object to the at least one further object only if there is a match between the calculated computation result and transferred computation result, and declaring the computation result as invalid for further transmissions (Column 5, lines 29-31, Column 8, lines 4-12).

The examiner notes that **Stellberger** teaches **"transmitting an item of information unidirectionally between the first object and the at least one further object"** as "Random number generator 24 provided in the lock unit generates an arbitrary but in individual cases definite random number x which serves as an input signal, for example x=438. If desired, the similar generation process can take place also in the key unit 10, as will be explained in greater detail in connection with flowchart II... The communication transceiver 27 of the lock unit now acts as a transmitter and transmits the input signal x to the communication transceiver 17 at the key unit, which now acts as a receiver. In this example, the transceivers 17 and 27 operate with infrared radiation 30. At this point the preliminary or control program is completed, and the actual main program, which includes the two-stage coding, is initiated" (Column 6, lines

60-67-Column 7, lines 1-8). The examiner further notes that **Stellberger** teaches **"calculating a computation result in the relevant receiving object from parts of the transmitted information"** as "Starting from the random input signal x, each unit of the device, that is the key unit and the lock unit, computes in a first stage, from the random input signal x, on the basis of functional equation y=f(x), which is the same for both units and which represents the algorithm for the computing operation in this first stage, the corresponding dependent variable y. This functional equation is a first code which in this first computation stage serves for the individualization of respective pairs of key and lock units which belong one to another and distinguishes the same with respect to other key and lock pairs. For example, if the functional equation is y=4.fourthroot.x+1.507, then when x=438 for example, the computation result in this first stage is y=6.08176" (Column 7, lines 9-23). The examiner further notes that **Stellberger** teaches **"comparing the calculated computation result with a computation result transferred with the information in the relevant receiving object"** as "Due to the succession of a plurality of working cycles an extraordinarily high degree of safety for distinguishing different pairs of key and lock parts is obtained. The comparison phase between the output signals produced in each working cycle is preferably made alternately in the key part and then in the lock part" (Column 4, lines 22-27) and "In the example of flowchart II it is assumed that the illustrated key and lock units belong to one another, and consequently the same computation result x1 is formed at either unit of the locking device" (Column 9, lines 32-36). The examiner further notes that **Stellberger** teaches **"authenticating the first object to the at least one further object only if there is a match between the calculated computation result and transferred computation result, and declaring the computation result as invalid for further transmissions"** as "On the other hand, when the two units agree with one another, that is when both output signals y' are identical, then the symbolic switching member 29 is in a position in which it releases an actuation pulse 38 which in the simple embodiment of the device of this invention immediately serves for the changeover of the bolt 35 at the lock unit. As soon as the position of the bolt is changed, the main program according to the flowchart I is completed" (Column 8, lines 4-12).

Stellberger does not explicitly teach:

B) providing no further communication between the first object and the at least one further object.

Schwegler, however, teaches **"providing no further communication between the first object and the at least one further object"** as "The actuation of one or more vehicle-protection functions via wireless communication channels between the electronic key and vehicle is a particularly significant feature. Modern vehicle-protection devices contain both electronically actuatable access-protection devices, such as door-locking systems or flap-locking systems and break-in/theft warning systems, as well as electronically actuatable vehicle immobilizing devices for protecting against unauthorized use by third parties. The actuation of the associated functional units is triggered by activating the associated key-end activation element, and involves a unidirectional or bidirectional exchange of data between the key and vehicle via the wireless communication channel, in order to check the authorization of the requesting key for the respective vehicle" (Column 1, lines 21-35) and "In this manner, a unidirectional or bidirectional data communication is established in order to actuate a vehicle-protection device" (Column 3, line 67-Column 4, lines 1-3).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Schwegler's** would have allowed **Stellberger's** provide convenient protection against incorrect operation, as noted by **Schwegler** (Column 3, lines 8-12).

Regarding claim 2, **Stellberger** further teaches a method comprising:

A) wherein the first object comprises a vehicle and the least further object comprises a key; and (Column 5, lines 58-61).

B) wherein the information is transmitted from the vehicle and received by the key (Column 5, lines 58-61).

The examiner notes that **Stellberger** teaches **"wherein the first object comprises a vehicle and the least further object comprises a key"** as "The lock unit 20 is secured to an object to be locked, for example a door 31 of a motor vehicle. The

key unit 10 has a convenient size matching the pocket, so that it can be readily carried by the user" (Column 5, lines 58-61). The examiner further notes that **Stellberger** teaches **"wherein the information is transmitted from the vehicle and received by the key"** as "The lock unit 20 is secured to an object to be locked, for example a door 31 of a motor vehicle. The key unit 10 has a convenient size matching the pocket, so that it can be readily carried by the user" (Column 5, lines 58-61).

Regarding claims 10 and 17, **Stellberger** does not explicitly teach a method comprising:

A) wherein the result is computed in at least one further object using a cryptological computation algorithm known there and a code word.

Schwegler, however, teaches **"wherein the result is computed in at least one further object using a cryptological computation algorithm known there and a code word"** as "As shown in the FIGURE, the invention comprises a plurality of access-authorizing and use-authorizing ignition keys for a given vehicle (20) which is indicated schematically. One such key (1) is shown, on the one hand in a position (1a) outside the vehicle, and on the other hand in a position (1b) inside the vehicle (20), inserted into the ignition lock (22) of the vehicle (20). The key (1) contains a control and logic unit (2) which has, inter alia, a memory component (9) for storing an access-authorization code and a memory component (10) for storing a use-authorization code" (Column 4, lines 23-33) and "In this way, the central locking system can be switched into the unlocked position and the break-in/theft warning system deactivated by a first activation of the remote-control button (4) on the access-authorizing key (1), in order to enter the vehicle. Conversely, after a person gets out of the vehicle, the central locking system can be switched back into the locked state and the alarm system activated, via a second activation of the remote-control button. The data communication which is used to actuate the one or more vehicle functions via this communication channel can take place in a unidirectional or bidirectional fashion, any desired cryptographic method being preferably used to encrypt the transmitted data information" (Column 5, lines 33-45).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Schwegler's** would have allowed **Stellberger's** provide convenient protection against incorrect operation, as noted by **Schwegler** (Column 3, lines 8-12).

Regarding claim 11, **Stellberger** teaches a method comprising:
A) transmitting an item of information unidirectionally between the vehicle and the key (Column 6, lines 60-67-Column 7, lines 1-8);
C) calculating a computation result in the key from parts of the transmitted information (Column 7, lines 9-23);
D) comparing the calculated computation result with a computation result transferred with the information, wherein the comparing is in the key (Column 4, lines 22-27, Column 9, lines 32-36); and
E) authenticating the vehicle if there is a match between the calculated computation result and the transferred computation result, and declaring the computation result as invalid for further transmissions (Column 5, lines 29-31, Column 8, lines 4-12).

The examiner notes that **Stellberger** teaches **"transmitting an item of information unidirectionally between the vehicle and the key"** as "Random number generator 24 provided in the lock unit generates an arbitrary but in individual cases definite random number x which serves as an input signal, for example x=438. If desired, the similar generation process can take place also in the key unit 10, as will be explained in greater detail in connection with flowchart II... The communication transceiver 27 of the lock unit now acts as a transmitter and transmits the input signal x to the communication transceiver 17 at the key unit, which now acts as a receiver. In this example, the transceivers 17 and 27 operate with infrared radiation 30. At this point the preliminary or control program is completed, and the actual main program, which includes the two-stage coding, is initiated" (Column 6, lines 60-67-Column 7, lines 1-8). The examiner further notes that **Stellberger** teaches **"calculating a computation result in the key from parts of the transmitted information"** as "Starting from the random input signal x, each unit of the device, that is the key unit and the lock unit,

computes in a first stage, from the random input signal x, on the basis of functional equation y=f(x), which is the same for both units and which represents the algorithm for the computing operation in this first stage, the corresponding dependent variable y. This functional equation is a first code which in this first computation stage serves for the individualization of respective pairs of key and lock units which belong one to another and distinguishes the same with respect to other key and lock pairs. For example, if the functional equation is y=4.fourthroot.x+1.507, then when x=438 for example, the computation result in this first stage is y=6.08176" (Column 7, lines 9-23). The examiner further notes that **Stellberger** teaches **"comparing the calculated computation result with a computation result transferred with the information, wherein the comparing is in the key"** as "Due to the succession of a plurality of working cycles an extraordinarily high degree of safety for distinguishing different pairs of key and lock parts is obtained. The comparison phase between the output signals produced in each working cycle is preferably made alternately in the key part and then in the lock part" (Column 4, lines 22-27) and "In the example of flowchart II it is assumed that the illustrated key and lock units belong to one another, and consequently the same computation result x1 is formed at either unit of the locking device" (Column 9, lines 32-36). The examiner further notes that **Stellberger** teaches **"authenticating the vehicle if there is a match between the calculated computation result and the transferred computation result, and declaring the computation result as invalid for further transmissions"** as "On the other hand, when the two units agree with one another, that is when both output signals y' are identical, then the symbolic switching member 29 is in a position in which it releases an actuation pulse 38 which in the simple embodiment of the device of this invention immediately serves for the changeover of the bolt 35 at the lock unit. As soon as the position of the bolt is changed, the main program according to the flowchart I is completed" (Column 8, lines 4-12).

Stellberger does not explicitly teach:

B) providing no further communication between the first object and the at least one further object.

Schwegler, however, teaches **"providing no further communication between the first object and the at least one further object"** as "The actuation of one or more vehicle-protection functions via wireless communication channels between the electronic key and vehicle is a particularly significant feature. Modern vehicle-protection devices contain both electronically actuatable access-protection devices, such as door-locking systems or flap-locking systems and break-in/theft warning systems, as well as electronically actuatable vehicle immobilizing devices for protecting against unauthorized use by third parties. The actuation of the associated functional units is triggered by activating the associated key-end activation element, and involves a unidirectional or bidirectional exchange of data between the key and vehicle via the wireless communication channel, in order to check the authorization of the requesting key for the respective vehicle" (Column 1, lines 21-35) and "In this manner, a unidirectional or bidirectional data communication is established in order to actuate a vehicle-protection device" (Column 3, line 67-Column 4, lines 1-3).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Schwegler's** would have allowed **Stellberger's** provide convenient protection against incorrect operation, as noted by **Schwegler** (Column 3, lines 8-12).

13. Claims 3-9, and 12-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Stellberger** (U.S. Patent 4,509,093) and in view of **Schwegler et al.** (U.S. Patent 5,808372) as applied to claims 1-2, 10-11, and 17 above, and further in view of **Kocher et al.** (U.S. Patent 6,381,699).

14. Regarding claim 3, **Stellberger** teaches a method comprising:

A) a random number (Column 5, lines 29-31)

Stellberger and **Schwegler** do not explicitly teach:

B) an incremental or decrementable item of data, wherein the incremental or decremental item of data is stored in the at least one further object if the calculated computation result matches the transferred computation result; and

C) wherein after each transmission of the information, regardless of a successful receipt, the item of data is incremented or decremented before new information is transmitted (Kocher, Column 9, lines 23-45).

Kocher, however, teaches **"an incremental or decrementable item of data, wherein the incremental or decremental item of data is stored in the at least one further object if the calculated computation result matches the transferred computation result"** as "sends other needed information (such as data or t) to the verifier" (Column 9, lines 23-45), and **"wherein after each transmission of the information, regardless of a successful receipt, the item of data is incremented or decremented before new information is transmitted"** as "if t matches, the verifier increments t" (Column 9, lines 23-45).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Kocher's** would have allowed **Stellberger's** and **Schwegler's** to provide a system of security that remains secure even if attackers gather some information about the system, as noted by **Kocher** (Column 2, lines 40-44).

Regarding claim 4, **Stellberger** teaches a method comprising:

A) a random number (Column 5, lines 29-31)

Stellberger and **Schwegler** do not explicitly teach:

B) an incremental or decrementable item of data, wherein the incremental or decremental item of data is stored in the key if the calculated computation result matches the transferred computation result; and

C) wherein after each transmission of the information, regardless of a successful receipt, the item of data is incremented or decremented before new information is transmitted (Kocher, Column 9, lines 23-45).

Kocher, however, teaches **"an incremental or decrementable item of data, wherein the incremental or decremental item of data is stored in the key if the calculated computation result matches the transferred computation result"** as "sends other needed information (such as data or t) to the verifier" (Column 9, lines 23-

45), and **"wherein after each transmission of the information, regardless of a successful receipt, the item of data is incremented or decremented before new information is transmitted"** as "if t matches, the verifier increments t" (Column 9, lines 23-45).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Kocher's** would have allowed **Stellberger's** and **Schwegler's** to provide a system of security that remains secure even if attackers gather some information about the system, as noted by **Kocher** (Column 2, lines 40-44).

Regarding claims 5-6, and 13, **Stellberger** and **Schwegler** do not explicitly teach a method comprising:

A) wherein a counter state or item of time data is transferred as the item of data that can be incremented.

Kocher, however, teaches **"a counter state or item of time data is transferred as the item of data that can be incremented"** as "counter t" (Column 9, line 24).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Kocher's** would have allowed **Stellberger's** and **Schwegler's** to provide a system of security that remains secure even if attackers gather some information about the system, as noted by **Kocher** (Column 2, lines 40-44).

Regarding claims 7 and 14, **Stellberger** and **Schwegler** do not explicitly teach a method comprising:

A) wherein the result is only calculated when the transferred item of data is greater than the stored item of data.

Kocher, however, teaches **"wherein the result is only calculated when the transferred item of data is greater than the stored item of data"** as "if the received value of t is larger than the internal value but the difference is not unreasonably large, it may be appropriate to accept the signature" (Column 9, lines 38-45).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Kocher's** would have allowed **Stellberger's** and **Schwegler's** to provide a system of security that remains secure even if attackers gather some information about the system, as noted by **Kocher** (Column 2, lines 40-44).

Regarding claims 8-9, and 15-16, **Stellberger** and **Schwegler** do not explicitly teach a method comprising:

A) wherein when the transferred result and the calculated result match, the incrementable item of data is increased so that the transferred result becomes invalid (Column 9, lines 23-45).

Kocher, however, teaches **"wherein when the transferred result and the calculated result match, the incrementable item of data is increased so that the transferred result becomes invalid"** as "if t matches" (Column 9, lines 38-45).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Kocher's** would have allowed **Stellberger's** and **Schwegler's** to provide a system of security that remains secure even if attackers gather some information about the system, as noted by **Kocher** (Column 2, lines 40-44).

Regarding claim 12, **Stellberger** teaches a method comprising:

A) a random number (Column 5, lines 29-31)

B) key (Column 5, lines 58-61)

Stellberger and **Schwegler** do not explicitly teach::

B) an incremental or decrementable item of data, wherein the incremental or decremental item of data is stored in the key if the calculated computation result matches the transferred computation result; and

C) wherein after each transmission of the information, regardless of a successful receipt, the item of data is incremented or decremented before new information is transmitted.

Kocher, however, teaches **"an incremental or decrementable item of data which is stored in the key if it matches the computation result, is transferred"** as "sends other needed information (such as data or t) to the verifier" (Column 9, lines 23-45), and **"wherein after each transmission of the information, regardless of a successful receipt, the item of data is incremented or decremented before new information is transmitted"** as "if t matches, the verifier increments t" (Column 9, lines 23-45).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Kocher's** would have allowed **Stellberger's** and **Schwegler's** to provide a system of security that remains secure even if attackers gather some information about the system, as noted by **Kocher** (Column 2, lines 40-44).

Response to Arguments

15. Applicant's arguments with respect to claims 1-17 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

16. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. PGPUB 20010052075 issued to **Feinberg** on 13 December 2001. The subject matter disclosed therein is pertinent to that of claims 1-17 (e.g., methods to provide device authentication).

U.S. Patent 5,767,784 issued to **Khamhorn** on 16 June 1998. The subject matter disclosed therein is pertinent to that of claims 1-17 (e.g., methods to provide authentication for vehicle entry).

U.S. Patent 5,365,225 issued to **Bachhuber** on 15 November 1994. The subject matter disclosed therein is pertinent to that of claims 1-17 (e.g., methods to provide unidirectional authentication).

U.S. Patent 5,596,641 issued to **Ohashi et al.** on 21 January 1997. The subject matter disclosed therein is pertinent to that of claims 1-17 (e.g., methods to provide remote authentication).

U.S. Patent 4,935,962 issued to **Austin** on 19 June 1990. The subject matter disclosed therein is pertinent to that of claims 1-17 (e.g., methods to provide unidirectional authentication).

U.S. Patent 4,723,121 issued to **van den Boom et al.** on 02 February 1988. The subject matter disclosed therein is pertinent to that of claims 1-17 (e.g., methods to provide authentication for vehicle entry).

Contact Information

17. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mahesh Dwivedi whose telephone number is (571) 272-2731. The examiner can normally be reached on Monday to Friday 8:20 am – 4:40 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tim Vo can be reached (571) 272-3642. The fax number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Mahesh Dwivedi
Patent Examiner
Art Unit 2168

November 24, 2008
/Mahesh H Dwivedi/
Examiner, Art Unit 2168
/Tim T. Vo/
Supervisory Patent Examiner, Art Unit 2168